party interception, then the need for a heightened level of transmission security [in] is contrasted to a more secure transmission environment, such as a dedicated communication channel. With respect to the sensitivity of the data, the transmission of sensitive data, such as user account information, voting data, and credit card information, might necessitate a higher value for [M] N, while less sensitive data, such as streaming video or the like, would allow a higher value for [M] N.

Please amend page 31, first full paragraph, to read as follows:

It should be understood that other quality of service issues may be factored into the above-[identified]described scheme to allow the server to modify the value [M] of N. In addition, other criteria similar to those set forth above[,] are contemplated and could be employed as part of the present invention.

AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions, and listings, of claims in the captioned Application:

Listing Of Claims:

Claim 1 (currently amended) A method for authenticating transferred data between a sender computer and a receiver computer of a service broker system for interactive monitoring and control of data to and from Internet enabled devices of a sender/receiver computer security system over [an open network] the Internet, the method comprising the steps of:

establishing a first secure transmission of data over the Internet between a virtual gateway of the sender computer and a Web site of the receiver computer, the computers being provided with browser programming for accessing and/or displaying files and other data between the sender and receiver computers over the Internet;

establishing at least one additional transmission of data between the sender computer gateway and the receiver computer Web site;

adaptively determining the number of additional transmissions between the sender computer gateway and the receiver computer Web site;

transmitting the data during at least one of the additional transmissions; and

authenticating each transmission in which data is transmitted.

Claim 2 (currently amended) The method [according to] set forth in claim 1, wherein the number of additional transmissions is adaptively selected, at least in part, based upon the performance overhead of the system.

Claim 3 (currently amended) The method [according to] set forth in claim 2, wherein the number of additional transmissions is variable and adaptively selected, at least in part, based upon monitored conditions.

Claim 4 (currently amended) The method [according to] set forth in claim 2, wherein the number of additional transmissions is adaptively selected, at least in part, based upon a set of criteria that are used in an algorithm to determine the number of additional transmissions, the criteria selected from the group consisting of the frequency of transmissions between the sender computer and receiver computer, the closeness of the sender computer to the source of the transactions, and the usage patterns of the [client] sender computer.

Claim 5 (currently amended) The method [according to] set forth in claim 4, wherein the algorithm is a statistical averaging algorithm.

Claim 6 (currently amended) The method [according to] set forth in claim 1, further comprising the step of transmitting at least one token to the receiver during the first secure transmission; wherein the data transmitting step further comprises transmitting at least one token along with the data; and wherein the authentication step comprises comparing the at least one token transmitted during the additional transmission to the at least one token transmitted during the first secure transmission to determine whether the transmission is authentic.

Claim 7 (currently amended) The method [according to] set forth in claim 6, wherein the at least one token comprises a preselected number of tokens.

Claim 8 (currently amended) The method [according to] set forth in claim 7, wherein the number of at least one transmissions corresponds to the preselected number of tokens.

Claim 9 (currently amended) The method [according to] set forth in claim 7, wherein the number of at least one transmissions is greater than the preselected number of tokens.

Claim 10 (currently amended) The method [according to] set forth in claim 7, wherein the number of at least one transmissions is less than the preselected number of tokens.

Claim 11 (currently amended) The method [according to] set forth in claim 6, wherein the at least one additional transmission is conducted over an unsecure or open connection.

Claim 12 (currently amended) The method [according to] set forth in claim 6, wherein the first secure transmission is encrypted.

Claim 13 (currently amended) The method [according to] set forth in claim 6, wherein the at least one additional transmission is sent in plaintext.

Claim 14 (currently amended) The method [according to] set forth in claim 6, further comprising the steps of transmitting a checksum value during the first transmission and having the receiver verify that the checksum value is accurate by comparing the transmitted value to a checksum value generated using a similar checksum algorithm.

Claim 15 (currently amended) The method [according to] set forth in claim 14, wherein the transmitted checksum value is based upon checksum values transmitted during the previous transmissions.

Please add the following new claims after claim 15:

- - 16. A method for authenticating transferred data between a sender computer and a receiver computer of a service broker system for interactive monitoring and control of data to and from one or more Internet enabled devices of a client/server security system over the Internet, the method comprising the steps of:

establishing a first secure transmission of data over the Internet between the sender computer and the receiver computer, each of the sender and receiver computers having a virtual gateway and/or a Web site for directing data therebetween, and browser

programming for accessing and/or displaying files and other data between the sender and receiver computers over the Internet;

establishing at least one additional transmission of data between the sender computer and the receiver computer;

adaptively determining the number of additional transmissions between the sender computer and the receiver computer;

transmitting the data during at least one of the additional transmissions; and

authenticating each transmission in which data is transmitted, wherein the number of additional transmissions is variable and adaptively selected, at least in part, based upon the performance overhead of the system, and, at least in part, based upon a set of criteria used in an algorithm to determine the number of additional transmissions, the criteria being selected from the group consisting of the frequency of transmissions between the sender computer and receiver computer, the closeness of the sender computer to the source of the transactions, and the usage patterns of the sender computer.

17. A method for authenticating transferred data between a sender computer and a receiver computer of a service broker system for interactive monitoring and control of data to and from Internet enabled devices of a sender/receiver computer security system over the Internet, the method comprising the steps of:

establishing a first secure transmission of data over the Internet between a Web site of the sender computer and a virtual gateway of the receiver computer, the